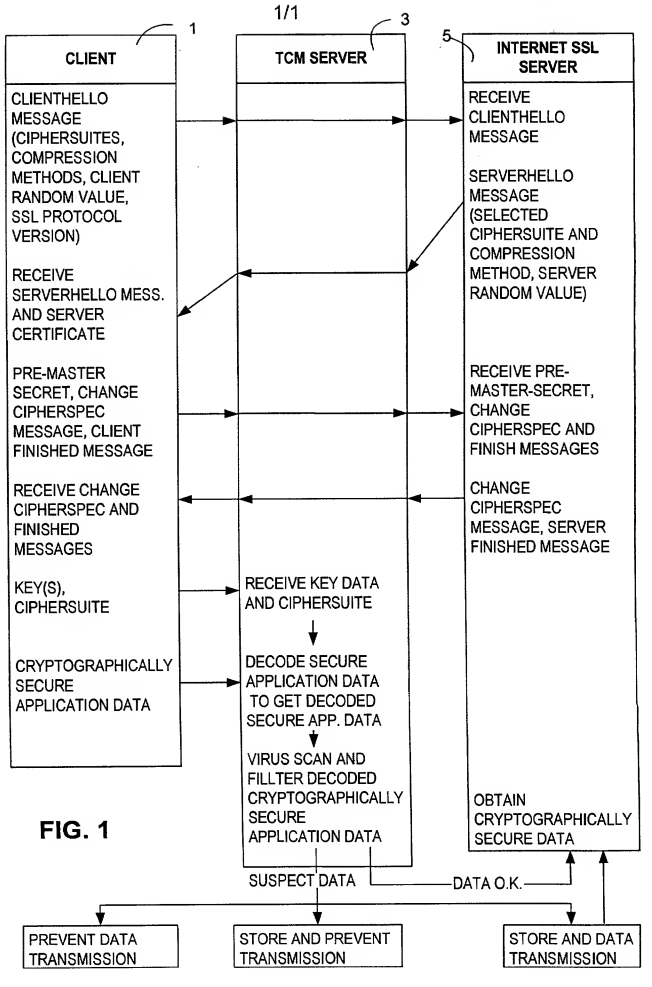
1
CLIENT
3
TCM SERVER
5
INTERNET SSL SERVER
CLIENTHELLO MESSAGE (CIPHERSUITES, COMPRESSION METHODS, CLIENT RANDOM VALUE, SSL PROTOCOL VERSION)
RECEIVE CLIENTHELLO MESSAGE
SERVERHELLO MESSAGE (SELECTED CIPHERSUITE AND COMPRESSION METHOD, SERVER RANDOM VALUE)
RECEIVE SERVERHELLO MESS. AND SERVER CERTIFICATE
PRE-MASTER SECRET, CHANGE CIPHERSPEC MESSAGE, CLIENT FINISHED MESSAGE
RECEIVE PRE-MASTER-SECRET, CHANGE CIPHERSPEC AND FINISH MESSAGES
RECEIVE CHANGE CIPHERSPEC AND FINISHED MESSAGES
CHANGE CIPHERSPEC MESSAGE, SERVER FINISHED MESSAGE
KEY(S), CIPHERSUITE
RECEIVE KEY DATA AND CIPHERSUITE
CRYPTOGRAPHICALLY SECURE APPLICATION DATA
DECODE SECURE APPLICATION DATA TO GET DECODED SECURE APP. DATA
VIRUS SCAN AND FILLTER DECODED CRYPTOGRAPHICALLY SECURE APPLICATION DATA
OBTAIN CRYPTOGRAPHICALLY SECURE DATA
SUSPECT DATA
DATA O.K.
PREVENT DATA TRANSMISSION
STORE AND PREVENT TRANSMISSION
STORE AND DATA TRANSMISSION

FIG. 1